

Listing of the Claims

A listing of the entire set of pending claims is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented): A method of generating an Authorized Domain (AD) comprises:
 - selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),
 - binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID),
 - binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and
 - binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by the domain identifier (Domain_ID),

thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN₁) that are authorized to access content items (C1, C2, ..., CN₂) of said Authorized Domain (AD)

wherein access to the at least one content item (C1, C2, ..., CN₂) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN₂) and the at least one user (P1, P2, ..., PN₁) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN₂) are linked to the same domain identifier (Domain_ID);

wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.
2. (Cancelled)

3. (Previously presented): A method according to claim 1, wherein the binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID) comprises:
 - obtaining or generating a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN₁) for a user

(P₁, P₂, ..., P_{N1}) thereby defining that the user is bound to the Authorized Domain (AD),
and/or in that

the binding at least one device (D₁, D₂, ..., D_M) to the domain identifier (Domain_ID) comprises:

obtaining or generating a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID₁, Dev.ID₂, ..., Dev.ID_M) for a device (D₁, D₂, ..., D_M) thereby defining that the device is bound to the Authorized Domain (AD).

4. (Previously presented): A method according to claim 3, wherein the binding at least one content item (C₁, C₂, ..., C_{N2}) to the Authorized Domain (AD) comprises:

binding a content item (C₁, C₂, ..., C_{N2}) to a User Right (URC₁, URC₂, ... URC_{N2}), where said User Right (URC₁, URC₂, ... URC_{N2}) is bound to a user (P₁, P₂, ..., P_{N1}) which is bound to the Authorized Domain (AD), and/or

binding a content item (C₁, C₂, ..., C_{N2}) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D₁, D₂, ..., D_M) which is bound to the Authorized Domain (AD), and/or

binding a content item (C₁, C₂, ..., C_{N2}) to a Domain Rights (DRC₁, DRC₂, ... DRC_{N2}), where said Domain Rights (DRC₁, DRC₂, ... DRC_{N2}) is bound to the Authorized Domain (AD).

5. (Cancelled)

6. (Previously presented): A method according to claim 4, wherein the User Right (URC₁, URC₂, ... URC_{N2}) or the Device Right (DevRC) or the Domain Rights (DRC₁, DRC₂, ... DRC_{N2}) comprises rights data (Rights Dat) representing which rights exists in relation to the at least one content item (C₁, C₂, ..., C_{N2}) bound to the User Right (URC₁, URC₂, ... URC_{N2}) or the Device Right (DevRC) or the Domain Rights (DRC₁, DRC₂, ... DRC_{N2}).

7. (Previously presented): A method according to claim 1, the method further comprises controlling access to a given content item bound to the Authorized Domain (AD) by a given device being operated by a given user, comprising:

 checking if the given user is bound to the same Authorized Domain (AD) as the given content item, or

 checking if the given device is bound to the same Authorized Domain (AD) as the given content item,

 and allowing access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (AD),

 or allowing access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (AD).

8. (Previously presented): A method according to claim 3, the method further comprises controlling access to a given content item (C1, C2, ..., CN₂), being bound to the Authorized Domain (AD) and having a unique content identifier (Cont_ID), by a given device being operated by a given user comprising:

 checking if the Domain Devices List (DDC) of the Authorized Domain (AD) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (AD) as the content item, and/or

 checking if the Domain User List (DUC) of the Authorized Domain (AD) comprises an identifier (Pers_ID) of the given user (P1, P2, ..., PN₁) thereby checking if the given user is bound to the same Authorized Domain (AD) as the content item,

 and allowing access to the given content item (C1, C2, ..., CN₂) by the given device (D1, D2, ..., DM) for any user if the given device is bound to the same Authorized Domain (AD) as the content item being accessed, and/or

 allowing access to the given content item (C1, C2, ..., CN₂) by any device including the given device for the given user if the given user is bound to the same Authorized Domain (AD) as the content item being accessed.

9. (Previously presented): A method according to claim 7, wherein the binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) comprises:

binding a content item (C1, C2, ..., CN₂) to a User Right (URC1, URC2, ... URCN₂), where said User Right (URC1, URC2, ... URCN₂) is bound to a user (P1, P2, ..., PN₁) which is bound to the Authorized Domain (AD), and

wherein the controlling access of a given content item further comprises:

checking that the User Right (URC1, URC2, ... URCN₂) for the given content item specifies that the given user (P1, P2, ..., PN₁) has a right to access the given content item (C1, C2, ..., CN₂) and only allowing access to the given content item (C1, C2, ..., CN₂) in the affirmative.

10. (Previously presented): A method according to claim 1, wherein every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Right (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

11. (Previously presented): A method according to claim 4, wherein

the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or

the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or

the User Right (URC1, URC2, ..., URCN₂) is implemented as or included in a User Right Certificate, and/or

the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or

the Domain Rights (DRC1, DRC2, ..., DRCN₂) is implemented as or included in a Domain Rights Certificate.

12. (Previously Presented): A system for generating an Authorized Domain (AD), the system comprising:

means for obtaining a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),
means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID),
means for binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and
means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by the domain identifier (Domain_ID),
thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN₁) that is authorized to access content items (C1, C2, ..., CN₂) of said Authorized Domain (AD)

wherein access to the at least one content item (C1, C2, ..., CN₂) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN₂) and the at least one user (P1, P2, ..., PN₁) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN₂) are linked to the same domain identifier (Domain_ID);

wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.

13. (Cancelled)

14. (Previously presented): A system according to claim 12, wherein the means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID) is adapted to obtain or generate a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN₁) for a user (P1, P2, ..., PN₁) thereby defining that the user is bound to the Authorized Domain (AD),

and/or in that

the means for binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID) is adapted to:

obtain or generate a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID1, Dev.ID2, ..., Dev.IDM) for a device (D1, D2, ..., DM) thereby defining that the device is bound to the Authorized Domain (AD).

15. (Previously presented): A system according to claim 14, wherein the means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) is adapted to:

bind a content item (C1, C2, ..., CN₂) to a User Right (URC1, URC2, ... URCN₂), where said User Right (URC1, URC2, ... URCN₂) is bound to a user (P1, P2, ..., PN₁) which is bound to the Authorized Domain (AD), and/or
bind a content item (C1, C2, ..., CN₂) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D1, D2, ..., DM) which is bound to the Authorized Domain (AD), and/or
bind a content item (C1, C2, ..., CN₂) to a Domain Rights (DRC1, DRC2, ... DRCN₂), where said Domain Rights (DRC1, DRC2, ... DRCN₂) is bound to the Authorized Domain (AD).

16. (Cancelled)

17. (Previously presented): A system according to claim 15, wherein the User Right (URC1, URC2, ... URCN₂) or the Device Right (DevRC) or the Domain Rights (DRC) comprises rights data (Rights Dat) representing which rights exists in relation to the at least one content item (C1, C2, ..., CN₂) bound to the User Right (URC1, URC2, ... URCN₂) or the Device Right (DevRC) or the Domain Rights (DRC1, DRC2, ... DRCN₂).

18. (Previously presented): A system according to claim 12, wherein the system further comprises means for controlling access to a given content item bound to the Authorized Domain (AD) by a given device being operated by a given user, where the means is adapted to:
check if the given user is bound to the same Authorized Domain (AD) as the given content item, or

check if the given device is bound to the same Authorized Domain (AD) as the given content item,
and allow access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (AD),
or allow access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (AD).

19. (Previously presented): A system according to claim 14, wherein the system further comprises means for controlling access to a given content item (C1, C2, ..., CN₂), being bound to the Authorized Domain (AD) and having a unique content identifier (Cont_ID), by a given device being operated by a given user, where the means is adapted to:

check if the Domain Devices List (DDC) of the Authorized Domain (AD) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (AD) as the content item, and/or
check if the Domain User List (DUC) of the Authorized Domain (AD) comprises an identifier (Pers_ID) of the given user (P1, P2, ..., PN₁) thereby checking if the given user is bound to the same Authorized Domain (AD) as the content item,
and allow access to the given content item (C1, C2, ..., CN₂) by the given device (D1, D2, ..., DM) for any user if the given device is bound to the same Authorized Domain (AD) as the content item being accessed, and/or
allow access to the given content item (C1, C2, ..., CN₂) by any device including the given device for the given user if the given user is bound to the same Authorized Domain (AD) as the content item being accessed.

20. (Previously presented): A system according to claim 18, wherein the means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) is adapted to:

bind a content item (C1, C2, ..., CN₂) to a User Right (URC1, URC2, ... URCN₂),
where said User Right (URC1, URC2, ... URCN₂) is bound to a user (P1, P2, ..., PN₁) which is bound to the Authorized Domain (AD), and

wherein the means for controlling access of a given content item is further adapted to further:

check that the User Right (URC1, URC2, ... URCN₂) for the given content item specifies that the given user (P1, P2, ..., PN₁) has a right to access the given content item (C1, C2, ..., CN₂) and only allowing access to the given content item (C1, C2, ..., CN₂) in the affirmative.

21. (Previously presented): A system according to claim 12, wherein every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Right (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

22. (Previously presented): A system according to claim 15, wherein

- the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or
- the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or
- the User Right (URC1, URC2, ..., URCN₂) is implemented as or included in a User Right Certificate, and/or
- the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or
- the Domain Rights (DRC1, DRC2, ..., DRCN₂) is implemented as or included in a Domain Rights Certificate.

23. (Currently Amended): A non-transitory computer readable medium having stored thereon instructions for causing one or more processing units to execute the method according to claim 1.